

# Online Security

or yes, you DO need unique passwords!



FEDERAL TRADE COMMISSION

# A Scummy Snapshot of 2022

(based on reports to Consumer Sentinel)

#FTCTopFrauds  
ftc.gov/data  
ReportFraud.ftc.gov

## Top Frauds



**2.4 million** fraud reports



**\$8.8 billion** reported lost

The number of reports is down.  
The amount lost is up.  
(2021: 2.9 million fraud reports, \$6.1 billion lost)

Losses to investment scams **more than doubled.**



**\$1.8 billion**

2021

**\$3.8 billion**

2022

Losses to business imposters soared.



**\$196 million**

2020

**\$453 million**

2021

**\$660 million**

2022

Scammers contacting people on social or by phone led to big losses



**\$1.2 billion** total lost

**Social media:** Highest overall reported losses



**\$1,400** median loss

**Phone calls:** Highest per person reported losses

<https://www.ftc.gov/new-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022>

# Step 1

Don't be afraid to admit that you've made a mistake  
or been the victim of a scammer!

# Step 2

Don't panic!



# Passwords

Yes, they are critically important!

# Passwords

1. Yes, you need unique passwords for all of your accounts
2. Yes, you really do need to remember them!
3. Should you allow your browser to remember your passwords?
4. Use a password manager or a password book



**KEEPER**  
Cybersecurity Starts Here™

**1Password**



**DASHLANE**



**LastPass**

# Passwords

## Characteristics of good passwords

- 15+ characters
- Mix of letters, capital letters, numbers, punctuation
- Not based on easily guessable information - your birth year, anniversary year, pets names, kids birthdays, etc.

## Tips for creating passwords

## How to recover lost passwords...



# Two-Factor or Multi-Factor Authentication

What is it? Do I need it?

# 2FA / MFA

It's difficult for a hacker to get access to your passwords and your device at the same time.

## Types of 2FA

- SMS (text messages)
- Authenticator app

# Secure Your Device

There's a lot of personal data in there!

# Secure Your Device

Use a PIN / passcode

Biometric logins – FaceID, fingerprint, etc.

Find/reset your device - “Find my device” for iOS and Android

iOS users: Turn off AirDrop or set to “contacts only”

Turn off Bluetooth if you’re not using it

# Malware

What is it? How do I avoid it?

# Malware

Adware

Ransomware

Potentially Unwanted Programs (PUPs)

Cryptocurrency miners

Spyware

Trojan Horse / 'backdoor' access

# Antivirus Programs

iOS users – you don't need one

Android users – maybe??

MacOS users – maybe??

Windows users - For most people, Windows Defender is  
Adequate!

Watch out for scammy antivirus programs, too!

# Avoiding malware & scams

- Never click a link in an email, text, etc.
  - Look carefully at WHO is sending the email
- Never let an unknown person into your device
- Don't believe caller ID or the "from" line in an email
- Be very cautious when entering financial data



# How to read a URL

Full web address (aka "URL")



[https://www.becybersafe.com/scams/EmailPhishing\\_Advanced.html](https://www.becybersafe.com/scams/EmailPhishing_Advanced.html)

Domain name

# How to read a URL

Two examples of scammers pretending to be PayPal:

<http://70.142.86.350/paypal.com/>

Web Address

Site Name

<http://paypal.account-update.mybank.com/>

Web Address

# Common Online Scams

Knowledge is power!

# Common Online Scams

1. ANYTHING that asks you to pay with gift card or crypto
2. Tech support scams
3. Phishing
4. Blackmail
5. Impersonators
6. Catfishing and romance scams
7. Cryptocurrency “investments”
8. Scammy businesses - including MLMs
9. People selling or buying things you’re trying to sell
  - a. Overpayments, fake check scams, going “off platform”

# Data Breaches

Now what?

# Data Breach - now what?

1. Change your passwords
2. Monitor your accounts carefully - banks, credit cards, investment accounts, etc.
3. Set up multi-factor authentication on all critical accounts
4. Freeze your credit (especially if you suspect your SSN or identification was breached)
5. Check your free credit reports

# Basic security tips


If it seems too good to be true  
or too scary to be true,  
it's probably not true!

# Basic tips for online security

1. Use unique, secure passwords
2. Use a password manager or book
3. Turn on 2FA/MFA whenever possible
4. Keep your devices updated
5. Secure your devices
6. Never let an unknown person into your device
7. Backup your data
8. ALWAYS be vigilant. (*Verify, don't trust*)
9. Never assume that you know who you're talking to!



# Basic tips for online security

10. Never make a decision in a hurry – scammers love to pressure you into making bad decisions
11. Be very cautious when entering financial data
  - a. Look for HTTPS or 
  - b. Use PayPal, Apple Pay or other secure pay service when you can
  - c. Watch out for “friends and family” payment apps like Venmo, Cash App, PayPal Friends and Family, etc.
12. Don't hesitate to admit when you've made a mistake!

**Don't forget  
to have fun!**



# Mercer Public Library

Teresa Schmidt, library director  
[director@mercerpubliclibrary.org](mailto:director@mercerpubliclibrary.org)

**715-476-2366**

<https://mercerpubliclibrary.org/program-and-class-handouts/>